IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS

JOSE ACEVEDO JR., individually and on behalf of all others similarly situated, Plaintiff, v. ILLINOIS DEPARTMENT OF INNOVATION AND TECHNOLOGY and PROGRESS SOFTWARE CORPORATION a/k/a PROGRESS, Defendants.	CASE NO. 2023-CV-003225 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jose Acevedo Jr. ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants Illinois Department of Innovation and Technology ("DoIT") and Progress Software Corporation a/k/a Progress ("Progress") (collectively, "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This putative class action arises from Defendants' negligent failure to implement and maintain reasonable cybersecurity procedures that resulted in a data breach, which was discovered in May or June 2023 (the "Data Breach").

2. In connection with the Data Breach, Progress, which develops and sells the MOVEit file-transfer program, and DoIT, an Illinois state agency specializing in

technology solutions, failed to properly secure and safeguard Plaintiff's and Class Members' protected personally identifiable information, including without limitation, full names, dates of birth, and Social Security numbers ("personal identifiable information" or "PII").[1]

3. In all, the Data Breach has impacted more than 17.5 million people, through more than 200 organizations, including pension fund management companies, corporations, government agencies, and law and accounting firms.[2]

4. At DoIT, there are approximately 390,000 individuals affected.[3]

5. Plaintiff brings this class action complaint to redress injuries related to the Data Breach, on behalf of himself and a nationwide class and an Illinois subclass of similarly situated persons.

6. Plaintiff asserts claims on behalf of a nationwide class against Defendants for negligence; negligence *per se*; invasion of privacy; violation of the Illinois' Personal Information Protection Act ("PIPA"), 815 ILCS 530/10(a); unjust enrichment; and declaratory judgment, and against DoIT for breach of implied contract and breach of the implied covenant of good faith and fair dealing.

7. Plaintiff seeks, among other things, compensatory damages, injunctive relief,

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).
[2] https://www.axios.com/2023/07/07/moveit-hack-200-target-millions-victims.
[3] https://doit.illinois.gov/news/press-release.26654.html.

attorneys' fees, and costs of suit.

PARTIES

8. Plaintiff Jose Acevedo Jr. is a citizen and resident of the State of Illinois whose personal identifying information was part of the June 2023 data breach that is the subject of this action. Plaintiff received a Notice of Data Incident letter ("Notice Letter") (attached hereto as **Exhibit A**), via U.S. mail, dated July 5, 2023.[4]

9. On information and belief, Defendant Illinois Department of Innovation and Technology is an Illinois state agency with its main office located at 201 W. Adams Street, Springfield, Illinois 62701.

10. On information and belief, Defendant Progress Software Corporation a/k/a Progress is a Delaware corporation with its principal place of business in located at 15 Wayside Rd. #400, Burlington, Massachusetts 01803.

11. Plaintiff brings this action on behalf of himself and on behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil Procedure 23.

JURISDICTION & VENUE

12. This Court has subject-matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

[4] *See* Ex. A.

13. This Court has general personal jurisdiction over Defendant Illinois Department of Innovation and Technology because it is an Illinois state agency whose main office is in this District.

14. This Court has specific personal jurisdiction over Defendant Progress Software Corporation because it sold its file transfer product MOVEit to customers in Illinois, including, as relevant to Plaintiff and the Class members, to DoIT.

15. Venue is proper in this Court because Defendant Illinois Department of Innovation and Technology has its headquarters in this District.

FACTUAL BACKGROUND

16. Progress develops and sells a variety of software for businesses, including the secure file transfer application MOVEit. Defendants advertises that more than 100,000 enterprises run business systems through its platforms, and 6 million business users work with apps running on Defendants' technologies.[5]

17. Progress's various business and government customers, including DoIT, retain sensitive information including, but not limited to, bank account information, addresses, driver's license numbers, dates of birth, and social security numbers, among other things, and use Progress's MOVEit product to securely transfer files containing that sensitive information.

18. Progress knew that they were a prime target for hackers given the significant amount of sensitive personal information processed through its customers' computer data

[5] https://investors.progress.com/?_ga=2.130524045.306488999.1689141297-1144817577.1689141297&_gl=1*klrbgt*_ga*MTE0NDgxNzU3Ny4xNjg5MTQxMjk3*_ga_9JSNBCSF54*MTY4OTE0MzY0MC4yLjAuMTY4OTE0MzY0NC41Ni4wLjA.

and storage systems.

19. DoIT is an Illinois agency that "guides technology solution delivery and support for the agencies in the executive branch of state government."[6]

20. DoIT specializes in technology solutions, including for, *inter alia*, IT networking, video conferring, and data security.[7]

21. Defendants' knowledge is underscored by the massive number of data breaches that have occurred in recent years.

22. Despite knowing the prevalence of data breaches, Defendants failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases.

23. Defendants had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. Defendants failed to undertake adequate analyses and testing of their own systems, training of their own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

24. On information and belief, the personal information Defendants' customers collect and which was impacted by the cybersecurity attack includes individual's name, date of birth, and social security number, among other personal, sensitive and confidential information.

[6] https://doit.illinois.gov/.
[7] https://doit.illinois.gov/services/catalog.html.

25. On or around July 5, 2023, DoIT mailed data breach notices to parties impacted by the MOVEit data breach. According to notice mailed to impacted individuals, the breach resulted in individual's name, address, and social security number being compromised and acquired by unauthorized actors. Plaintiff received a copy of the July 5, 2023, data breach notice letter, via United States mail service, confirming that his personal identifying information was part of the Data Breach.

26. Upon information and belief, the hackers responsible for the Data Breach stole the personal information of many of Defendants' customers, including Plaintiff's. Because of the nature of the breach and of the personal information stored or processed by Defendants' customers, Plaintiff is informed and believes that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiff is informed and believes that criminals would have no purpose for hacking Defendants' software other than to exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the coveted personal information stored or processed by Defendants' customers.

27. The personal information exposed by Defendants as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals.

28. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

29. When malicious actors infiltrate companies and copy and exfiltrate the personal information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

30. The information compromised in this unauthorized cybersecurity attack involves sensitive personal identifying information, which is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Whereas here, the information compromised is difficult and highly problematic to change—particularly Social Security numbers.

31. Once personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personal information being harvested from the victim, as well as personal information from family, friends, and colleagues of the original victim.

32. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personal information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

33. The high value of PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

$200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[10]

34. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

35. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the- dark-web-how-much-it-costs/ (last accessed July 12, 2023).

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-.
personal-information-is-selling-for-on-the-dark-web/ (last accessed July 12, 2023).

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 12, 2023).

36. Identity thieves can use PII, such as that of Plaintiff and Class Members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

37. The ramifications of Defendants' failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Plaintiff's and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

38. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed July 12, 2023).

39. When cyber criminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may have exposed Plaintiff and Class Members.

40. And data breaches are preventable.[12] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[13] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[14]

41. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[15]

42. Federal and state governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

---

[12] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[13] *Id.* at 17.
[14] *Id.* at 28.
[15] *Id.*

43. According to the FTC, the need for data security should be factored into all business decision-making.[16] In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[17] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

44. Also, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[18]

45. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personal information, treating the failure to employ

[16] *See* Federal Trade Commission, Start with Security (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed July 12, 2023).

[17] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 12, 2023).

[18] *See id.*

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

46. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. Defendants' failure to safeguard against a cybersecurity attack is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cybersecurity routinely identify companies such as Defendants' customers that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain. Accordingly, Defendants knew or should have known that its customers were a prime target for hackers.

48. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[19]

49. Upon information and belief, Defendants did not encrypt Plaintiff's and Class Members' personal information involved in the Data Breach.

[19] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach*, Security, Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-datq-breach (last accessed July 12, 2023).

50. As detailed above, Progress is a large, sophisticated software company with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

51. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that its customer's network servers were protected against unauthorized intrusions when using the MOVEit program; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to its customers, and therefore Plaintiff and Class members, prompt and accurate notice of the Data Breach.

Plaintiff's Facts

52. DoIT received highly sensitive PII from Plaintiff in connection with DoIT's services.

53. As a result of the vulnerability in Progress's MOVEit product, Plaintiff's information provided to DoIT was among the data accessed by an unauthorized third party in the Data Breach.

54. At all times herein relevant, Plaintiff is and was a member of the nationwide class and the Illinois subclass alleged herein.

55. Plaintiff's PII was exposed in the Data Breach because Defendants stored and/or controlled Plaintiff's PII at the time of the Data Breach.

56. Plaintiff received a letter from DoIT, dated July 5, 2023, stating that his name, address, and social security number, which was in the possession, custody and/or control of Defendants, was involved in the Data Breach (the "Notice").

57. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

58. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII.

59. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, being placed in the hands of unauthorized third parties/criminals.

60. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

61. Plaintiff's and Class Members' personal identifying information, including their names and social security numbers, were in the possession, custody and/or control of Defendants. Plaintiff believed that Defendants would protect and keep his personal identifying information protected, secure and safe from unlawful disclosure.

62. Plaintiff and Class Members have spent and will continue to spend time and

effort monitoring his accounts to protect themselves from identity theft. Plaintiff and Class Members remain concerned for their personal security and the uncertainty of what personal information was exposed to hackers and/or posted to the dark web.

63. As a direct and foreseeable result of Defendants' negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiff and all Class Members, have suffered harm in that their sensitive personal information has been exposed to cybercriminals and they have an increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the breach.

64. Plaintiff and Class Members are especially concerned about the misappropriation of their Social Security numbers. Social security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's social security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security

number and assuming your identity can cause a lot of problems.[20]

65. Furthermore, Plaintiff and Class Members are well aware that their sensitive personal information, including social security numbers and potentially banking information, risks being available to other cybercriminals on the dark web. Accordingly, all Plaintiff and Class Members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the data breach.

66. Additionally, Plaintiff and Class Members have incurred and/or will incur, out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

CLASS ACTION ALLEGATIONS

67. Plaintiff brings this action on behalf of himself and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiff seeks to represent the following class and subclass:

> **Nationwide Class**. All persons in the United States whose personal information was compromised in or as a result of Defendants' data breach discovered by Defendants in May or June 2023 (the "Class").
>
> **Illinois Subclass.** All persons residing in Illinois whose personal information was compromised in or as a result of Defendants' data breach discovered by Defendants in May or June 2023 (the "Illinois Subclass").

Excluded from the classes are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which Defendants has a controlling interest; all individuals who make a timely request to be

[20] *Identify Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 12, 2023).

excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserves the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

69. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

70. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of Class Members at issue has not been determined, Plaintiff believes the cybersecurity breach affected hundreds of thousands of individuals nationwide.

71. Commonality: There are questions of law and fact common to Plaintiff and the class that predominate over any questions affecting only the individual members of the class. The common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants owed a duty to Plaintiff and Class Members to exercise due care in collecting, storing, processing, and safeguarding their personal information being transferred through the MOVEit program;

b. Whether Defendants breached those duties;

c. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of Class Members being transferred through the MOVEit program;

d. Whether Defendants acted negligently in connection with the vulnerabilities in the MOVEit program that allowed unauthorized access to Plaintiff's and Class Members' personal information;

e. Whether Defendants knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' personal information secure and prevent loss or misuse of that personal information;

f. Whether Defendants adequately addressed and fixed the vulnerabilities in the MOVEit program which permitted the data breach to occur;

g. Whether Defendants caused Plaintiff and Class Members damages;

h. Whether the damages Defendants caused to Plaintiff and Class Members includes the increased risk and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;

i. Whether Plaintiff and Class Members are entitled to credit monitoring and other monetary relief;

j. Whether Defendants' failure to implement and maintain reasonable security procedures and practices constitutes negligence;

k. Whether Defendants' failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;

l. Whether Defendants' failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

m. Whether DoIT breached an implied contract with Plaintiff and Class members; and

n. Whether DoIT breached the implied covenant of good faith and fair dealing with Plaintiff and Class members;

72. Typicality. The claims of the named Plaintiff are typical of the claims of the Class Members because all had their personal information compromised as a result of Defendants' failure to implement and maintain reasonable security measures and the consequent data breach.

73. Adequacy of Representation. Plaintiff will fairly and adequately represent the interests of the class. Counsel who represent Plaintiff are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.

74. Superiority and Manageability. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiff is not practicable, and questions of law and fact common to Plaintiff predominate over any questions affecting only Plaintiff. Plaintiff has been damaged and is entitled to recovery by reason of Defendants' unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation make it impracticable for most Class Members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely

on behalf of himself or himself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as Defendants' records will readily enable the Court and parties to ascertain affected companies and their employees.

75. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants has acted or refused to act on grounds generally applicable to the class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

76. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to maintain security in the transfer of their personal information;

b. Whether Defendants breached that legal duty to Plaintiff and Class Members to exercise due care in maintaining security in the transfer of their personal information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information compromised in the breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring, injunctive relief, and/or statutory damages, as a result of Defendants' wrongful conduct as alleged herein.

CAUSES OF ACTION

COUNT 1
Negligence
(On behalf of Plaintiff and the Class against Defendants)

77. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

78. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in securing the data being transferred through the MOVEit product from being compromised, stolen, accessed, and/or misused by unauthorized persons.

79. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices.

80. Defendants' duties included a duty to design, maintain, and test its security systems to ensure that Plaintiff's and Class Members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding intrusions to its networks, and to promptly,

properly, and fully notify its clients, Plaintiff, and Class Members of any data breach.

81. Defendants' duties to use reasonable care arose from several sources, including but not limited to those described below.

82. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants also knew that it was more likely than not Plaintiff and other Class Members would be harmed.

83. Defendants' duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendants.

84. Various FTC publications and data security breach orders further form the basis of Defendants' duty. According to the FTC, the need for data security should be factored into all business decision making.[21] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for

[21] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

fundamental data security principles and practices for business.[22] Those guidelines recommend, among other things, encryption of all data being stored or transferred.

85. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

86. The FBI has also issued guidance on best practices with respect to data security that also form the basis of Defendants' duty of care, as described above.[23]

87. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' personal information, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' personal information from disclosure.

88. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their personal information.

89. Defendants breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiff and Class

---

[22] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[23] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed July 12, 2023).

Members; (b) prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry; (e) timely disclose that Plaintiff's and Class Members' personal information in Defendants' possession had been or was reasonably believed to have been stolen or compromised; (f) failing to comply fully even with its own purported security practices.

90. Defendants knew or should have known of the risks of transferring personal information through its product and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of Defendants' operations further shows that Defendants knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief, this is but one of the several vulnerabilities that plagued Defendants' systems and led to the data breach.

91. Through Defendants' acts and omissions described in this complaint, including Defendants' failure to provide adequate security and its failure to protect the personal information of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' personal information.

92. Defendants further failed to timely and accurately disclose to clients, Plaintiff, and Class Members that their personal information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web. Plaintiff and Class

Members could have taken action to protect their personal information if they were provided timely notice.

93. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their personal information would not have been compromised.

94. Plaintiff and Class Members relied on Defendants to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

95. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory and nominal damages, in an amount to be proven at trial. As a result of Defendants' failure to protect Plaintiff's and Class Members' personal information, Plaintiff's and Class Members' personal information has been accessed by malicious cybercriminals. Plaintiff 'and the Class Members' injuries include:

a. theft of their personal information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and

identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

d. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

e. damages to and diminution of value of their personal information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and the Class Members' data against theft and not allow access and misuse of their data by others;

f. continued risk of exposure to hackers and thieves of their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;

g. loss of the inherent value of their personal information;

h. the loss of the opportunity to determine for themselves how their personal information is used; and

i. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

96. In connection with the conduct descried above, Defendants acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class Members would suffer if their highly sensitive and confidential personal information, including but not limited to name, address, and social security numbers was access by unauthorized third parties.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Class against Defendants)

97. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

98. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendants. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

99. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach.

100. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

101. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was meant to protect.

102. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

103. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory and nominal damages, in an amount to be proven at trial.

COUNT III
Invasion of Privacy
(On behalf of Plaintiff and the Class against Defendants)

104. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

105. The State of Illinois recognizes the tort of Invasion of Privacy:

> The elements of the cause of action typically are stated as: (1) the Defendants committed an unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering.

Busse v. Motorola, Inc., 351 Ill. App. 3d 67, 71, 813 N.E.2d 1013, 1017 (2004).

106. Plaintiff and Class Members had a reasonable expectation of privacy in the PII that Defendants mishandled.

107. Defendants' conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

108. By intentionally failing to keep Plaintiff's and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

109. Defendants knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendants' intentional actions highly offensive and objectionable.

110. Defendants invaded Plaintiff and Class Members' right to privacy and intruded into Plaintiff's and Class Members' seclusion by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

111. Defendants intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

112. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

113. In failing to protect Plaintiff's and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

114. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

COUNT IV
Violations Of Illinois' Personal Information Protection Act ("PIPA"), 815 ILCS 530/10(a)
(On behalf of Plaintiff and the Illinois Subclass against Defendant Progress)

115. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

116. Section 10(b) of PIPA states, in pertinent part:

> "[a]ny data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does

> not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

815 ILCS 530/10(b).

117. Defendant Progress is "data collector" as defined by the statute; it is a software company that "handles, collects, disseminates, or otherwise deals with nonpublic personal information. 815 ILCS 530/5.

118. Plaintiff's and the Illinois Subclass Members' claims are based on their status as an "owner" of their personal information.

119. Defendant Progress failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

120. Section 45 of Illinois's Personal Information Protection Act requires entities who maintain or store "personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

121. Defendant's conduct violated the Personal Information Protection Act.

122. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII , but Defendants failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated.

123. Defendant should have known and anticipated that data breaches were on the rise and that software companies were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

124. As a result of Defendant Progress's violation of the Personal Information Protection Act, Plaintiff and the Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the Class against Defendants)

125. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

126. Plaintiff and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable PII.

127. Defendants enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

128. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

129. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

130. Defendants acquired the monetary benefit and PII, through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

131. If Plaintiff and Class Members knew that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants or let Defendants collect, store, and/or maintain their PII.

132. Plaintiff and Class Members have no adequate remedy at law.

133. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

j. theft of their personal information;

k. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

l. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

m. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

n. damages to and diminution of value of their personal information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and the Class Members' data against theft and not allow access and misuse of their data by others;

o. continued risk of exposure to hackers and thieves of their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;

p. loss of the inherent value of their personal information;

q. the loss of the opportunity to determine for themselves how their personal information is used; and

r. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

134. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

135. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT VI
Breach of Implied Contract
(On Behalf of Plaintiff and the Class Against DoIT)

136. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

137. Through its course of conduct, DoIT, Plaintiff and Class Members entered into implied contracts for DoIT to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

138. DoIT required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining DoIT's services.

139. DoIT solicited and invited Plaintiff and Class Members to provide their PII as part of Defendants' regular business practices. Plaintiff and Class Members accepted DoIT's offers and provided their PII to DoIT for services.

140. Plaintiff and Class Members provided and entrusted their PII to DoIT. In so doing, Plaintiff and Class Members entered into implied contracts with DoIT by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

141. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to DoIT, in exchange for, amongst other things, the protection of their PII.

142. Plaintiff and Class Members fully performed their obligations under the implied contracts with DoIT.

143. DoIT breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

144. As a direct and proximate result of DoIT's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT VII
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class Against DoIT)

145. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

146. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

147. Plaintiff and Class Members have complied with and performed all conditions of their contracts with DoIT.

148. DoIT breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

149. DoIT acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT VII
Declaratory Judgment
(On behalf of Plaintiff and the Class against Defendants)

150. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

151. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as the ones alleged here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

152. An actual controversy has arisen in the wake of the Defendants data breach regarding its present and prospective common law and other duties to reasonably safeguard

consumers' personal identifying information being transferred through its secure file transfer program, and regarding whether Defendants is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their personal information. Plaintiff continues to suffer injury as a result of the compromise of their personal information and remains at imminent risk that further compromises of his personal information will occur in the future.

153. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' personal information, including Plaintiff's and Class Members' personal information, to timely notify them of a data breach under the common law, Section 5 of the FTC Act; and

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' personal information.

154. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' personal information.

155. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff will not have an adequate remedy at law because many of the resulting

injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

156. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

157. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and the thousands of Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, the Nationwide Class and the Illinois Subclass, prays for the following relief:

1. An order certifying the nationwide Class and Illinois Subclass as defined above pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiff is a proper class representative and appointing Plaintiff's counsel as class counsel;
2. Permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial, in excess of $5,000,000;

4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;

5. A declaration of right and liabilities of the parties;

6. Costs of suit;

7. Reasonable attorneys' fees;

8. Pre- and post-judgment interest at the maximum legal rate;

9. Distribution of any monies recovered on behalf of members of the class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendants from retaining the benefits of their wrongful conduct; and

10. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative class and subclass, hereby demands a trial by jury on all issues of fact or law so triable.

DATED: July 14, 2023

Respectfully Submitted,

By:*/s/ Jeff Ostrow*

Jeff Ostrow
Kristen Lake Cardoso
Steven Sukert
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

cardoso@kolawyers.com
sukert@kolawyers.com

Andrew J. Shamis
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 400
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Gary M. Klinger
MILBERG COLEMAN BRYSON LLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Attorneys for Plaintiff Jose Acevedo Jr. and the Putative Class